

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-072184

(43)Date of publication of application : 04.03.2004

(51)Int.Cl. H04L 9/32
H04L 9/08
H04L 9/14
H04N 7/08
H04N 7/081

(21)Application number : 2002-225034

(71)Applicant : NIPPON HOSO KYOKAI <NHK>

(22)Date of filing : 01.08.2002

(72)Inventor : OGAWA KAZUTO

GOSHI SEIICHI

MUROTA ITSURO

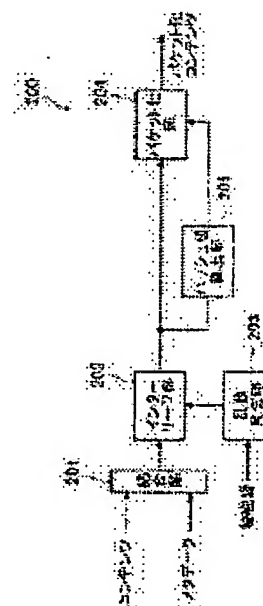
OTAKE TAKESHI

(54) DATA TAMPERING PREVENTION APPARATUS AND PROGRAM THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data tampering prevention apparatus capable of making the tampering of contents or metadata difficult and to provide a program therefor.

SOLUTION: The data tampering prevention apparatus is provided with: a coupling means 201 for coupling received contents and metadata to each other to produce coupled data; a random number generating means 203 for using a private key to generate a random number; an interleave means 202 for modifying a data arrangement in the couple data to produce rearrangement data; a hash value calculation means 205 for calculating a hash value in response to data of a prescribed part of the rearranged data; and a packetizing means 204 for converting the data of the prescribed part of the rearranged data in response to the hash value to produce packetized contents, and the interleave means 202 is configured to decide a data stream being an object of revising the data arrangement on the basis of the random number.



(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2004-72184

(P2004-72184A)

(43) 公開日 平成16年3月4日 (2004. 3. 4)

(51) Int. Cl. ⁷	F I	テーマコード (参考)
H04L 9/32	H04L 9/00 675A	5C063
H04L 9/08	H04N 7/08 Z	5J104
H04L 9/14	H04L 9/00 601B	
H04N 7/08	H04L 9/00 641	
H04N 7/081		

審査請求 未請求 請求項の数 9 O L (全 18 頁)

(21) 出願番号	特願2002-225034 (P2002-225034)	(71) 出願人	000004352 日本放送協会 東京都渋谷区神南2丁目2番1号
(22) 出願日	平成14年8月1日 (2002. 8. 1)	(74) 代理人	100072604 弁理士 有我 軍一郎
		(72) 発明者	小川 一人 東京都世田谷区砧一丁目10番11号 日 本放送協会 放送技術研究所内
		(72) 発明者	合志 清一 東京都世田谷区砧一丁目10番11号 日 本放送協会 放送技術研究所内
		(72) 発明者	室田 逸郎 東京都世田谷区砧一丁目10番11号 日 本放送協会 放送技術研究所内

最終頁に続く

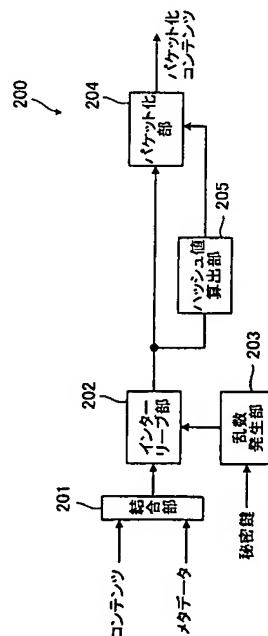
(54) 【発明の名称】 データ改竄防止装置およびそのプログラム

(57) 【要約】

【課題】 コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止装置およびそのプログラムを提供すること。

【解決手段】 入力されるコンテンツとメタデータとを結合して結合データを生成する結合手段201と、秘密鍵を用いて乱数を発生する乱数発生手段203と、結合データ内のデータ配列を変更して配列入替データを生成するインターリーブ手段202と、配列入替データの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出手段205と、ハッシュ値に応じて配列入替データの所定部分のデータを変換してパケット化コンテンツを生成するパケット化手段204とを備え、インターリーブ手段202がデータ配列を変更する対象のデータ列を乱数に基づいて決定する構成を有している。

【選択図】 図2



【特許請求の範囲】

【請求項 1】

入力されるコンテンツとメタデータとを結合して結合データを生成する結合手段と、前記結合データ内のデータ配列を変更して配列入替データを生成するインターリーブ手段と、前記配列入替データの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出手段と、前記ハッシュ値に応じて前記配列入替データの所定部分のデータを変換してパケット化コンテンツを生成するパケット化手段とを備えたことを特徴とするデータ改竄防止装置。

【請求項 2】

入力されるメタデータの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出手段と、入力されたコンテンツの所定部分のデータを前記ハッシュ値に応じて変換して変換データを生成し前記変換データと前記メタデータと結合して結合変換データを生成するパケット化手段と、前記結合変換データ内のデータ配列を変更してパケット化コンテンツを生成するインターリーブ手段とを備えたことを特徴とするデータ改竄防止装置。

【請求項 3】

前記データ改竄防止装置は、さらに秘密鍵を用いて乱数を発生する乱数発生手段を備え、前記インターリーブ手段は、前記データ配列を変更する対象のデータ列を前記乱数に基づいて決定することを特徴とする請求項 1 または請求項 2 記載のデータ改竄防止装置。

【請求項 4】

請求項 1 記載のデータ改竄防止装置によって生成されたパケット化コンテンツに応じて前記データ改竄防止装置が算出するハッシュ値と同一のハッシュ値を算出するハッシュ値算出手段と、前記ハッシュ値に応じて前記パケット化コンテンツを逆変換して前記データ改竄防止装置が生成する前記配列入替データと同一の配列入替データに戻す逆パケット化手段と、前記配列入替データのデータ配列を変更して前記データ改竄防止装置が生成する結合データと同一の結合データに戻すインターリーブ手段と、前記結合データを前記コンテンツと前記メタデータとに分離するメタデータ分離手段とを備えたことを特徴とするデータ改竄防止装置。

【請求項 5】

請求項 2 記載のデータ改竄防止装置によって生成されたパケット化コンテンツのデータ配列を変更して前記データ改竄防止装置が生成する結合変換データと同一の結合変換データに戻すインターリーブ手段と、前記結合変換データを前記データ改竄防止装置によって変換された変換データと前記メタデータとに分離するメタデータ分離手段と、前記メタデータに応じて前記データ改竄防止装置が算出するハッシュ値と同一のハッシュ値を算出するハッシュ値算出手段と、前記ハッシュ値に応じて前記データ改竄防止装置によって変換された変換データを逆変換して元のコンテンツを生成する逆パケット化手段とを備えたことを特徴とするデータ改竄防止装置。

【請求項 6】

前記データ改竄防止装置は、さらに請求項 1 または請求項 2 記載のデータ改竄防止装置に入力される秘密鍵を用いて請求項 1 または請求項 2 記載のデータ改竄防止装置が発生する乱数と同一の乱数を発生する乱数発生手段を備え、前記インターリーブ手段は、前記乱数に基づいてデータ配列を元に戻す対象のデータ列を決定することを特徴とする請求項 4 または請求項 5 記載のデータ改竄防止装置。

【請求項 7】

コンピュータに、入力されるコンテンツとメタデータとを結合して結合データを生成する結合ステップと、前記結合データ内のデータ配列を変更して配列入替データを生成するインターリーブステップと、前記配列入替データの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出ステップと、前記ハッシュ値に応じて前記配列入替データの所定部分のデータを変換してパケット化コンテンツを生成するパケット化ステップとを実行させることを特徴とするデータ改竄防止プログラム。

【請求項 8】

10

20

30

40

50

コンピュータに、入力されるメタデータの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出ステップと、入力されたコンテンツの所定部分のデータを前記ハッシュ値に応じて変換して変換データを生成し前記変換データと前記メタデータと結合して結合変換データを生成するパケット化ステップと、前記結合変換データ内のデータ配列を変更してパケット化コンテンツを生成するインターリーブステップとを実行させることを特徴とするデータ改竄防止プログラム。

【請求項 9】

前記データ改竄防止プログラムは、さらにコンピュータに、秘密鍵を用いて乱数を発生する乱数発生ステップを実行させ、前記インターリーブステップで、前記データ配列を変更する対象のデータ列を前記乱数に基づいて決定することを特徴とする請求項 7 または請求項 8 記載のデータ改竄防止プログラム。

10

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、コンテンツの流通過程における、コンテンツの改竄またはコンテンツに付加されるメタデータ等の改竄を困難にするためのデータ改竄防止装置およびそのプログラムに関する。

【0002】

【従来の技術】

従来、コンテンツの流通過程において、コンテンツにメタデータと呼ばれる付加情報を加えて配信する場合、コンテンツのヘッダとして、メタデータを付加し、一つのコンテンツパケットとして配信することが一般的であった。ここで、メタデータは、これが付加されたコンテンツに関するものであり、ヘッダ部分に組み込まれているため、コンテンツと容易に分離可能であり、改竄が容易であった。

20

【0003】

そのため、コンテンツに対応するメタデータを容易に取得できないようにするために、コンテンツにメタデータを付加せず、コンテンツの配信とメタデータの配信のタイミングをずらすことや、コンテンツをパッケージにして配送してメタデータをネットワーク経由で配信する等の別系統でコンテンツとメタデータを届けること等が行われている。この場合も、メタデータとコンテンツとは一体ではなく、始めから分離されている。

30

【0004】

また、コンテンツやメタデータの改竄防止のために、コンテンツやメタデータを暗号化してから配信することが一般に行われている。しかし、この場合も、コンテンツとメタデータは別々に暗号化され、容易に分離できるような構造となっていた。

【0005】

【発明が解決しようとする課題】

しかしながら、従来の技術では、コンテンツとメタデータとは分離できるものであり暗号化されていても個別に解読することができるため、メタデータを不正に改竄することが容易であるという問題があった。その結果、メタデータとして、例えば、コンテンツの視聴制御情報、視聴回数制限情報、コピー回数制御情報等が含まれる場合に、これらを改竄し、制限回数を超えた視聴や、コピー制御を無効にしたコピーが可能となることがあり、分離されたコンテンツのみが不正にコピーされるおそれがあった。

40

【0006】

本発明は、かかる問題を解決するためになされたもので、その目的は、コンテンツとメタデータに分離困難な変換処理を施すことによって、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止装置およびそのプログラムを提供することにある。

【0007】

【課題を解決するための手段】

以上の点を考慮して、請求項 1 に係る発明は、入力されるコンテンツとメタデータとを結

50

合して結合データを生成する結合手段と、前記結合データ内のデータ配列を変更して配列入替データを生成するインターリーブ手段と、前記配列入替データの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出手段と、前記ハッシュ値に応じて前記配列入替データの所定部分のデータを変換してパケット化コンテンツを生成するパケット化手段とを備えた構成を有している。

【0008】

この構成により、コンテンツとメタデータとを結合して一体としてから、データ配列を変更しデータを変換してパケット化コンテンツを生成するため、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止装置を実現できる。

【0009】

また、請求項2に係る発明は、入力されるメタデータの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出手段と、入力されたコンテンツの所定部分のデータを前記ハッシュ値に応じて変換して変換データを生成し前記変換データと前記メタデータと結合して結合変換データを生成するパケット化手段と、前記結合変換データ内のデータ配列を変更してパケット化コンテンツを生成するインターリーブ手段とを備えた構成を有している。

【0010】

この構成により、コンテンツとメタデータとを結合して一体としてから、データ配列を変更しデータを変換してパケット化コンテンツを生成するため、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止装置を実現できる。

【0011】

また、請求項3に係る発明は、請求項1または請求項2において、前記データ改竄防止装置は、さらに秘密鍵を用いて乱数を発生する乱数発生手段を備え、前記インターリーブ手段は、前記データ配列を変更する対象のデータ列を前記乱数に基づいて決定する構成を有している。

【0012】

この構成により、秘密鍵を用いて発生したハッシュ値を用いてデータ配列の変更を行っているため、データのわずかな改竄が行われた場合でも、ハッシュ値が大きく変化するため、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止装置を実現できる。

【0013】

また、請求項4に係る発明は、請求項1記載のデータ改竄防止装置によって生成されたパケット化コンテンツに応じて前記データ改竄防止装置が算出するハッシュ値と同一のハッシュ値を算出するハッシュ値算出手段と、前記ハッシュ値に応じて前記パケット化コンテンツを逆変換して前記データ改竄防止装置が生成する前記配列入替データと同一の配列入替データに戻す逆パケット化手段と、前記配列入替データのデータ配列を変更して前記データ改竄防止装置が生成する結合データと同一の結合データに戻すインターリーブ手段と、前記結合データを前記コンテンツと前記メタデータとに分離するメタデータ分離手段とを備えた構成を有している。

【0014】

この構成により、コンテンツとメタデータとを結合して一体としてからパケット化されたコンテンツを逆変換によって再生するため、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止装置を実現できる。

【0015】

また、請求項5に係る発明は、請求項2記載のデータ改竄防止装置によって生成されたパケット化コンテンツのデータ配列を変更して前記データ改竄防止装置が生成する結合変換データと同一の結合変換データに戻すインターリーブ手段と、前記結合変換データを前記データ改竄防止装置によって変換された変換データと前記メタデータとに分離するメタデータ分離手段と、前記メタデータに応じて前記データ改竄防止装置が算出するハッシュ値と同一のハッシュ値を算出するハッシュ値算出手段と、前記ハッシュ値に応じて前記デー

10

20

30

40

50

タ改竄防止装置によって変換された変換データを逆変換して元のコンテンツを生成する逆パケット化手段とを備えた構成を有している。

【0016】

この構成により、コンテンツとメタデータとを結合して一体としてからパケット化されたコンテンツを逆変換によって再生するため、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止装置を実現できる。

【0017】

また、請求項6に係る発明は、請求項4または請求項5において、前記データ改竄防止装置は、さらに請求項1または請求項2記載のデータ改竄防止装置に入力される秘密鍵を用いて請求項1または請求項2記載のデータ改竄防止装置が発生する乱数と同一の乱数を発生する乱数発生手段を備え、前記インターリーブ手段は、前記乱数に基づいてデータ配列を元に戻す対象のデータ列を決定する構成を有している。

10

【0018】

この構成により、パケット化コンテンツの生成に用いられる秘密鍵と同一の秘密鍵を用いて発生した同一のハッシュ値を用いて逆変換するため、データのわずかな改竄が行われた場合でも、ハッシュ値が大きく変換し、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止装置を実現できる。

【0019】

また、請求項7に係る発明は、コンピュータに、入力されるコンテンツとメタデータとを結合して結合データを生成する結合ステップと、前記結合データ内のデータ配列を変更して配列入替データを生成するインターリーブステップと、前記配列入替データの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出ステップと、前記ハッシュ値に応じて前記配列入替データの所定部分のデータを変換してパケット化コンテンツを生成するパケット化ステップとを実行させる構成を有している。

20

【0020】

この構成により、コンテンツとメタデータとを結合して一体としてから、データ配列を変更しデータを変換してパケット化コンテンツを生成するため、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止プログラムを実現できる。

【0021】

また、請求項8に係る発明は、コンピュータに、入力されるメタデータの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出ステップと、入力されたコンテンツの所定部分のデータを前記ハッシュ値に応じて変換して変換データを生成し前記変換データと前記メタデータと結合して結合変換データを生成するパケット化ステップと、前記結合変換データ内のデータ配列を変更してパケット化コンテンツを生成するインターリーブステップとを実行させる構成を有している。

30

【0022】

この構成により、コンテンツとメタデータとを結合して一体としてから、データ配列を変更しデータを変換してパケット化コンテンツを生成するため、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止プログラムを実現できる。

【0023】

また、請求項9に係る発明は、請求項7または請求項8において 前記データ改竄防止プログラムは、さらにコンピュータに、秘密鍵を用いて乱数を発生する乱数発生ステップを実行させ、前記インターリーブステップで、前記データ配列を変更する対象のデータ列を前記乱数に基づいて決定する構成を有している。

40

【0024】

この構成により、秘密鍵を用いて発生したハッシュ値を用いてデータ配列の変更を行っているため、データのわずかな改竄が行われた場合でも、ハッシュ値が大きく変換するため、コンテンツまたはメタデータの改竄を困難にすることが可能なデータ改竄防止プログラムを実現できる。

【0025】

50

【発明の実施の形態】

以下、本発明の実施の形態に係るデータ改竄防止装置およびそのプログラムについて、添付図面を用いて説明する。

(第1の実施の形態)

図1は、本発明の第1の実施形態に係るデータ改竄防止システム100の構成を示すブロック図である。データ改竄防止システム100は、プロバイダ側に構成されるシステムであり、ユーザ側のユーザ端末110からの要求をインターネット120を介して受信し、要求に応じたコンテンツとメタデータとをパケット化して配信するシステムである。

【0026】

図1に示すデータ改竄防止システム100では、制御中継装置101がユーザ端末110からインターネット120を介して送信されたコンテンツ配信要求を受信し、制御中継装置101の制御の下、コンテンツパケット化サーバ105が要求されたコンテンツをコンテンツサーバ103から、このコンテンツに付加するメタデータをメタデータサーバ104から、受け取ってパケット化されたコンテンツ（以下、単にパケット化コンテンツという。）を作成し、コンテンツ配信サーバ106がこのパケット化コンテンツをユーザ端末110に配信する。

【0027】

制御中継装置101は、ユーザ端末110からインターネット120を介して送信されたコンテンツ配信要求を受信し、要求されたコンテンツに応じたパケット化コンテンツの生成から配送までの各処理を実行させるために各サーバの制御および中継処理を行うようになっている。

イントラネット102は、これに接続されるサーバ間のデータ通信を可能とするLAN（Local Area Network）等のネットワークである。

【0028】

コンテンツサーバ103は、コンテンツを記憶しているサーバであり、ユーザ端末110によって要求されたコンテンツをコンテンツパケット化サーバ105に送信する。なお、コンテンツは暗号化されていても、暗号化されていなくてもよい。

メタデータサーバ104は、メタデータを記憶しているサーバであり、ユーザ端末110によって要求されたコンテンツに付加するメタデータをコンテンツパケット化サーバ105に送信する。なお、メタデータは暗号化されていても暗号化されていなくてもよい。

【0029】

コンテンツパケット化サーバ105は、コンテンツサーバ103から送信されたコンテンツと、メタデータサーバ104から送信されたメタデータとを合成してパケット化コンテンツを生成する。

コンテンツ配信サーバ106は、コンテンツパケット化サーバ105が生成したパケット化コンテンツをコンテンツの配信を要求したユーザ端末110に制御中継装置101経由で配信する。

【0030】

図2は、本発明の第1の実施形態に係るデータ改竄防止装置であるコンテンツパケット化サーバの構成を示すブロック図である。図2では、図1に示すコンテンツパケット化サーバ105をデータ改竄防止装置（コンテンツパケット化サーバ）200として表す。データ改竄防止装置（コンテンツパケット化サーバ）200は、入力されるコンテンツとメタデータとを結合して結合データを生成する結合部201、秘密鍵を用いて乱数を発生する乱数発生部203、結合データ内のデータ配列を変更して配列入替データを生成するインターリーブ部202、配列入替データの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出部205、およびハッシュ値に応じて配列入替データの所定部分のデータを変換してパケット化コンテンツを生成するパケット化部204を有する。

【0031】

結合部201は、入力されたコンテンツおよびメタデータを結合して1つの結合データにするようになっている。

10

20

30

40

50

インターリーブ部202は、結合部201から出力されるビットの並びである結合データ内のデータ配列の順番を入れ替え、配列入替データを生成するようになっている。入れ替えにおいて乱数発生部203が発生した乱数に基づいて入れ替え位置を決定することができる。なお、乱数を用いずに予め決められた入れ替え位置のデータを入れ替えることもできるが、入替位置を探索されることによって乱数を用いた場合よりも改竄の危険性が高い。

【0032】

乱数発生部203は、乱数を発生するようになっている。乱数発生部203には、秘密鍵が入力され、秘密鍵を用いて乱数を発生するのでもよい。乱数の発生は秘密鍵に基づいて行われ、かかる技術は公知であるため、その説明を省略する。また、秘密鍵としては、任意の数値にするのでも良い。

【0033】

パケット化部204は、インターリーブ部202によってデータ配列が入れ替えられて得られたデータである配列入替データが入力され、この配列入替データの所定位置のデータをハッシュ値算出部205から受け取ったハッシュ値に応じて変換してパケット化コンテンツを生成し、生成したパケット化コンテンツを外部に出力するようになっている。

【0034】

ハッシュ値算出部205は、配列入替データ内の所定部分のデータに応じたハッシュ値を算出し、パケット化部204に出力するようになっている。ハッシュ値は、ハッシュ関数を用いて生成されるデータであり、ハッシュ値の算出技術は公知であるため説明を省略する。

【0035】

以下、図3および図4を用いて本発明の第1の実施の形態に係るデータ改竄防止方法について説明する。

本発明の第1の実施の形態に係るデータ改竄防止方法では、入力されたコンテンツとメタデータとが結合部201によって結合されて一つの結合データが生成され（ステップS301）、入力された秘密鍵に応じて乱数が乱数発生部203によって発生され（ステップS302）、発生した乱数に基づいて結合データ内のデータ配列の入替えがインターリーブ部202によって行なわれ配列入替データが生成され（ステップS303）、配列入替データ410における予め決められた位置を占めるデータ411に応じてハッシュ値420が生成され（ステップS304）、データ411以外の所定のデータ412がデータ412とハッシュ値との演算により変換されパケット化コンテンツ430が生成される（ステップS305）。

【0036】

以下に、パケット化コンテンツの生成（ステップS305）について、図4を用いて具体的に説明する。パケット化コンテンツ430の生成において、処理対象の入力データ（配列入替データ）は、その内の所定部分のデータがハッシュ値を用いて変換されるものである。ここで、図4に示すように配列入替データ410が構成され、ハッシュ値の算出に用いられるデータ411が「1011111・・・」であり、データ411に基づいて算出されたハッシュ値420が「00101100」であり、変換対象のデータ列412の一例が「11000110」であるとする。

【0037】

図4には、上記の演算として排他的論理和を適用した例が示されている。この例では、変換対象のデータ列412の一例である「11000110」とハッシュ値420である「00101100」との排他的論理和の計算が行われて変換後のデータ列431「11101010」が算出され、データ412に置き換えられてパケット化コンテンツ430内に配置される。

【0038】

なお、上記の演算は、排他的論理和に限られず、可換な演算であればよい。また、ビット単位の演算でも複数ビットをまとめた演算であってもよい。ただし、変換対象のデータ列

412は、ハッシュ値の算出に用いられるデータ列以外の部分とする。コンテンツの再生を可能とするためである。

【0039】

また、本発明の第1の実施の形態では、上記のステップS301からS305までの各ステップでの処理を行うデータ改竄防止方法について説明したが、これらのステップS301からS305までの各ステップでの処理を含むデータ改竄防止動作を実行させるためのデータ改竄防止プログラムを生成し、そのプログラムに基づいて、コンピュータに、これらのステップS301からS305までの各ステップでの処理を含むデータ改竄防止動作を実行させることも可能である。

【0040】

以上説明したように、本発明の第1の実施の形態に係るデータ改竄防止装置およびプログラムは、コンテンツとメタデータとを結合して一体としてから、データ配列を変更しデータを変換してパケット化コンテンツを生成するため、コンテンツまたはメタデータの改竄を困難にすることができる。

また、秘密鍵を用いて発生したハッシュ値を用いてデータ配列の変更を行っているため、データのわずかな改竄が行われた場合でも、ハッシュ値が大きく変化するため、コンテンツまたはメタデータの改竄を困難にすることができる。

【0041】

(第2の実施の形態)

図5は、本発明の第2の実施形態に係るデータ改竄防止装置の構成を示すブロック図である。図5に示すデータ改竄防止装置500は、本発明の第1の実施の形態に係るデータ改竄防止システム100にコンテンツの配信を要求するユーザ端末110に含まれ、データ改竄防止システムから送信されユーザ端末110が受信したパケット化コンテンツを再生するための装置である。

【0042】

データ改竄防止装置500は、本発明の第1の実施の形態に係るデータ改竄防止装置によって生成されたパケット化コンテンツに応じてデータ改竄防止装置が算出するハッシュ値と同一のハッシュ値を算出するハッシュ値算出部501、算出したハッシュ値に応じてパケット化コンテンツを逆変換して本発明の第1の実施の形態に係るデータ改竄防止装置が生成する配列入替データと同一の配列入替データに戻す逆パケット化部502、本発明の第1の実施の形態に係るデータ改竄防止装置に入力される秘密鍵を用いて、このデータ改竄防止装置が発生する乱数と同一の乱数を発生する乱数発生部504、配列入替データのデータ配列を変更して本発明の第1の実施の形態に係るデータ改竄防止装置が生成する結合データと同一の結合データに戻すインターリーブ部503、および復元された結合データをコンテンツとメタデータとに分離するメタデータ分離部505を有する。

【0043】

ハッシュ値算出部501は、入力されたパケット化コンテンツの予め決められた位置に配置されたデータに応じたハッシュ値を算出するようになっている。上記の予め決められた位置としては、パケット化コンテンツの送信側でハッシュ値の算出に用いたデータが配置された位置として予め決められた位置をいい、ハッシュ値算出部501は、同一の送信側と同一のハッシュ値を算出するものである。

【0044】

逆パケット化部502は、受信したパケット化コンテンツをハッシュ値算出部501が発生したハッシュ値を用いてパケット化を解いて元の配列入替データとするようになっている。これは、上記のパケット化の処理を逆方向に行うことによって実現される。なお、ハッシュ値を演算して得られたデータを元のデータに変換するには、同一のハッシュ値を用いた逆演算を行うことで実現できる。排他的論理和を例にとると、逆演算も排他的論理和となる。

【0045】

インターリーブ部503は、逆パケット化部502によってパケット化が解かれたデータ

10

20

30

40

50

である配列入替データ内のデータ配列の順番を元に戻し、元の結合データを生成するようになっている。元に戻す処理は、乱数発生部504が発生した乱数に基づいてデータが入れ替えられた位置を算出することによって実現できる。なお、乱数を発生させてデータの入れ替えを行っていない場合は、予め決められた位置のデータの配列を入れ替えるものとする。

【0046】

乱数発生部504は、乱数を発生するようになっている。なお、データ改竄防止装置（コンテンツパッケージ化サーバ）200の乱数発生部203が秘密鍵を用いる場合、乱数発生部504にも、これと同一の秘密鍵が入力され、秘密鍵を用いてデータ改竄防止装置（コンテンツパッケージ化サーバ）200の乱数発生部203が発生する乱数と同一の乱数を発生する。

10

【0047】

メタデータ分離部505は、インターリーブ部503によって生成された元の結合データからメタデータを分離し、コンテンツとメタデータとを別々に出力するようになっている。

以上の各構成部は、データ改竄防止装置（コンテンツパッケージ化サーバ）200によって行われた処理の逆変換を行うものであり、逆変換によって元のコンテンツとメタデータを再生するものである。

【0048】

以下、図6を用いて本発明の第2の実施の形態に係るデータ改竄防止方法について説明する。

20

本発明の第2の実施の形態に係るデータ改竄防止方法では、入力されたパッケージ化コンテンツの所定部分のデータに応じたハッシュ値がハッシュ値算出部501によって算出され（ステップS601）、パッケージ化コンテンツの予め決められた位置のデータが逆パッケージ化部502によってハッシュ値を用いて逆演算処理されてパッケージ化が解かれ（ステップS602）、パッケージ化が解かれたデータの配列を戻すためのデータが乱数発生部504によって発生され（ステップS603）、パッケージ化が解かれたデータがインターリーブ部503によって元のコンテンツ等のデータ配列に戻され（ステップS604）、元のコンテンツ等のデータ配列に変換されたデータからメタデータがメタデータ分離部505によって分離される（ステップS605）。

30

【0049】

本発明の第2の実施の形態に係るデータ改竄防止装置およびそのプログラムでは、ハッシュ値とコンテンツ等との演算を行ってコンテンツ等を変換することにより、コンテンツの改竄に対する対策が行われている。ハッシュ値を求めるための、SHA1のようなハッシュ関数は入力データ内のほんの小さな部分が変化しても、その出力値が大きく変化する関数である。このため、もし、メタデータに改竄が行われた場合、そのハッシュ値は大きく変化する。この大きく変化してしまったハッシュ値とパッケージ化されたコンテンツの演算を行い、もとのコンテンツを復元することは困難である。これにより、メタデータの改竄防止、コンテンツの改竄防止を行うことができる。

【0050】

また、本発明の第2の実施の形態では、上記のステップS601からS605までの各ステップでの処理を行うデータ改竄防止方法について説明したが、これらのステップS601からS605までの各ステップでの処理を含むデータ改竄防止動作を実行させるためのデータ改竄防止プログラムを生成し、そのプログラムに基づいて、コンピュータに、これらのステップS601からS605までの各ステップでの処理を含むデータ改竄防止動作を実行させることも可能である。

40

【0051】

以上説明したように、本発明の第2の実施の形態に係るデータ改竄防止装置およびプログラムは、コンテンツとメタデータとを結合して一体としてからパッケージ化されたコンテンツを逆変換によって再生するため、コンテンツまたはメタデータの改竄を困難にすること

50

ができる。

【0052】

(第3の実施の形態)

図7は、本発明の第3の実施形態に係るデータ改竄防止装置であるコンテンツパッケージ化サーバの構成を示すブロック図である。図7では、図1に示すコンテンツパッケージ化サーバ105をデータ改竄防止装置(コンテンツパッケージ化サーバ)700として表す。データ改竄防止装置(コンテンツパッケージ化サーバ)700は、入力されるメタデータの所定部分のデータに応じたハッシュ値を算出するハッシュ値算出部701、入力されたコンテンツの所定部分のデータをハッシュ値に応じて変換して変換データを生成し変換データとメタデータと結合して結合変換データを生成するパッケージ化部702、乱数を発生する乱数発生部704、および結合変換データ内のデータ配列を変更してパッケージ化コンテンツを生成するインターリーブ部703を有する。

10

【0053】

ハッシュ値算出部701は、入力されたメタデータに応じたハッシュ値を算出し、パッケージ化部702に出力するようになっている。ハッシュ値の算出には、メタデータの一部を使用するのでも、全部を使用するのでも良い。

パッケージ化部702は、ハッシュ値算出部701からハッシュ値が入力され、このハッシュ値を用いてコンテンツ内の予め決められた部分のデータを変換して変換データを生成し、変換データとメタデータとを結合して結合変換データするようになっている。

【0054】

20

この変換について図8を用いて説明する。図8に示すように入力コンテンツ810が与えられ、ハッシュ値820が「00101100」と得られたとする。入力コンテンツ810の内、「11000110」の部分811を変換対象の部分とすると、変換は、例えば部分811「11000110」とハッシュ値820「00101100」との排他的論理和をとることによって行われる。

【0055】

なお、この演算についても上記の第1の実施の形態と同様に排他的論理和に限られず、可換な演算であれば他の演算であってもよい。また、コンテンツ内で、ハッシュ値を用いて変換する部分は予め定められたものであってもよいが、乱数を発生させ、発生した乱数に応じた部分を変換するようにしても良く、ビット単位の演算でも複数ビットまとめた演算であってもよい。

30

【0056】

インターリーブ部703は、パッケージ化部702から出力された結合変換データ内のデータ配列の順番を入れ替えるようになっている。入れ替えにおいて乱数発生部704が発生した乱数に基づいて入れ替え位置を決定することができる。なお、乱数を用いずに予め決められた入れ替え位置のデータを入れ替えることもできるが、入れ替え位置を感知されることによって乱数を用いた場合よりも改竄の危険性が高い。

【0057】

乱数発生部704は、乱数を発生し、発生した乱数をインターリーブ部703に出力するようになっている。乱数発生部704には、秘密鍵が入力され、秘密鍵を用いて乱数を発生するのでもよい。乱数の発生は秘密鍵に基づいて行われ、かかる技術は公知であるため、その説明を省略する。また、秘密鍵としては、任意の数値にするのでも良い。

40

以上の構成によりインターリーブ部703からはパッケージ化コンテンツが出力されるようになっている。

【0058】

以下、図9を用いて本発明の第3の実施の形態に係るデータ改竄防止方法について説明する。

本発明の第3の実施の形態に係るデータ改竄防止方法では、入力されたメタデータに応じたハッシュ値がハッシュ値算出部701によって生成され(ステップS901)、入力されたコンテンツの所定部分がパッケージ化部702によってハッシュ値に応じて変換され(

50

ステップS902)、入力された秘密鍵に応じて乱数が乱数発生部704によって発生され(ステップS903)、発生した乱数に基づいて結合変換データ内のデータ列の入替えがインターリーブ部703によって行なわれパケット化コンテンツが生成される(ステップS904)。

【0059】

また、本発明の第3の実施の形態では、上記のステップS901からS904までの各ステップでの処理を行うデータ改竄防止方法について説明したが、これらのステップS901からS904までの各ステップでの処理を含むデータ改竄防止動作を実行させるためのデータ改竄防止プログラムを生成し、そのプログラムに基づいて、コンピュータに、これらのステップS901からS904までの各ステップでの処理を含むデータ改竄防止動作

10

【0060】

以上説明したように、本発明の第3の実施の形態に係るデータ改竄防止装置およびプログラムは、コンテンツとメタデータとを結合して一体としてから、データ配列を変更しデータを変換してパケット化コンテンツを生成するため、コンテンツまたはメタデータの改竄を困難にすることができる。

また、秘密鍵を用いて発生したハッシュ値を用いてデータ配列の変更を行っているため、データのわずかな改竄が行われた場合でも、ハッシュ値が大きく変化するため、コンテンツまたはメタデータの改竄を困難にすることができる。

【0061】

20

(第4の実施の形態)

図10は、本発明の第4の実施形態に係るデータ改竄防止装置の構成を示すブロック図である。図10に示すデータ改竄防止装置1000は、本発明の第3の実施の形態に係るデータ改竄防止システム100にコンテンツの配信を要求するユーザ端末110に含まれ、本発明の第3の実施の形態に係るデータ改竄防止システムから送信されユーザ端末110が受信したパケット化コンテンツを再生するための装置である。

【0062】

データ改竄防止装置1000は、乱数を発生させる乱数発生部1002、発生した乱数に基づいてパケット化コンテンツのデータ配列を元に戻すインターリーブ部1001、インターリーブ部1001から出力されたデータの内メタデータを分離するメタデータ分離部1003、分離されたメタデータに応じたハッシュ値を算出するハッシュ値算出部1004、およびメタデータ分離部1003により分離され出力されたデータであってハッシュ値を用いて変換されたコンテンツを元のコンテンツに戻す逆パケット化部1005を有する。

30

【0063】

インターリーブ部1001は、乱数発生部1002が発生した乱数に基づいてパケット化コンテンツのデータ配列を元に戻すようになっている。元に戻す処理は、乱数発生部1002が発生した乱数に基づいてデータが入れ替えられた位置を算出するものとする。なお、乱数を発生させてデータの入れ替えを行っていない場合は、予め決められた位置のデータの配列を入れ替えるものとする。

40

【0064】

乱数発生部1002は、乱数を発生するようになっている。なお、データ改竄防止装置(コンテンツパケット化サーバ)700の乱数発生部704が秘密鍵を用いる場合、乱数発生部1002にも、これと同一の秘密鍵が入力され、秘密鍵を用いてデータ改竄防止装置(コンテンツパケット化サーバ)700の乱数発生部704が発生する乱数と同一の乱数を発生する。

【0065】

メタデータ分離部1003は、インターリーブ部1001によって元のデータ配列に戻されたデータからメタデータを分離し、分離したメタデータはハッシュ値算出部1004および外部に出力され、残りのデータ(以下、変換コンテンツという。)は、逆パケット化

50

部 1 0 0 5 に出力されるようになっている。

【 0 0 6 6 】

ハッシュ値算出部 1 0 0 4 は、メタデータ分離部 1 0 0 3 から入力されたメタデータの予め決められた位置に配置されたデータに応じたハッシュ値を算出するようになっている。上記の予め決められた位置としては、メタデータの送信側で上記のようにハッシュ値を算出したデータが配置された位置として予め決められた位置をいう。

【 0 0 6 7 】

逆パケット化部 1 0 0 5 は、メタデータ分離部 1 0 0 3 から入力された変換コンテンツをハッシュ値算出部 1 0 0 4 が発生したハッシュ値を用いて逆変換し、元のコンテンツとするようになっている。これは、本発明の第 3 の実施の形態のパケット化処理を逆方向に行うことによって実現される。なお、逆変換は、変換の際に生成したハッシュ値と同一のハッシュ値を用いて逆演算を行うことにより実現できる。排他的論理和を例にとると、逆演算も排他的論理和となる。

【 0 0 6 8 】

以上の各構成部は、データ改竄防止装置（コンテンツパケット化サーバ）7 0 0 によって行われた処理の逆変換を行うものであり、逆変換によって元のコンテンツとメタデータを再生するものである。

【 0 0 6 9 】

以下、図 1 1 を用いて本発明の第 4 の実施の形態に係るデータ改竄防止方法について説明する。

本発明の第 4 の実施の形態に係るデータ改竄防止方法では、本発明の第 3 の実施の形態に係るデータ改竄防止装置 7 0 0 の乱数発生部 7 0 4 が用いる秘密鍵と同一の秘密鍵を用いて、同一の乱数が乱数発生部 1 0 0 2 によって発生され（ステップ S 1 1 0 1）、ステップ S 1 1 0 1 で発生した乱数に基づいてパケット化コンテンツのデータ配列がインターリーブ部 1 0 0 1 によって元に戻され（ステップ S 1 1 0 2）、ステップ S 1 1 0 2 で元のデータ配列に戻されたデータからメタデータがメタデータ分離部 1 0 0 3 によって分離されてメタデータと変換コンテンツが生成され（ステップ S 1 1 0 3）、ステップ S 1 1 0 3 で生成されたメタデータの予め決められた位置に配置されたデータに応じたハッシュ値がハッシュ値算出部 1 0 0 4 によって算出され（ステップ S 1 1 0 4）、ステップ S 1 1 0 3 で生成された変換コンテンツがステップ S 1 1 0 4 で発生したハッシュ値を用いて逆パケット化部 1 0 0 5 によって逆変換されて元のコンテンツに戻される（ステップ S 1 1 0 5）。

【 0 0 7 0 】

本発明の第 4 の実施の形態に係るデータ改竄防止装置およびそのプログラムでは、ハッシュ値とコンテンツ等との演算を行ってコンテンツ等を変換することにより、コンテンツの改竄に対する対策が行われている。ハッシュ値を求めるための、SHA1 のようなハッシュ関数は入力データ内のほんの小さな部分が変化しても、その出力値が大きく変化する関数である。このため、もし、メタデータに改竄が行われた場合、そのハッシュ値は大きく変化する。この大きく変化してしまったハッシュ値とパケット化されたコンテンツの演算を行い、もとのコンテンツを復元することは不可能である。これにより、メタデータの改竄防止、コンテンツの改竄防止を行うことができる。

【 0 0 7 1 】

また、本発明の第 4 の実施の形態では、上記のステップ S 1 1 0 1 から S 1 1 0 5 までの各ステップでの処理を行うデータ改竄防止方法について説明したが、これらのステップ S 1 1 0 1 から S 1 1 0 5 までの各ステップでの処理を含むデータ改竄防止動作を実行させるためのデータ改竄防止プログラムを生成し、そのプログラムに基づいて、コンピュータに、これらのステップ S 1 1 0 1 から S 1 1 0 5 までの各ステップでの処理を含むデータ改竄防止動作を実行させることも可能である。

【 0 0 7 2 】

以上説明したように、本発明の第 4 の実施の形態に係るデータ改竄防止装置およびプログ

ラムは、コンテンツとメタデータとを結合して一体としてからパケット化されたコンテンツを逆変換によって再生するため、コンテンツまたはメタデータの改竄を困難にすることができる。

【0073】

【発明の効果】

以上説明したように、本発明は、コンテンツとメタデータに分離困難な変換処理を施すことによって、コンテンツまたはメタデータの改竄を防止することが可能なデータ改竄防止装置およびそのプログラムを提供することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係るデータ改竄防止システムの構成を示す図である。 10

【図2】本発明の第1の実施形態に係るデータ改竄防止装置の構成を示すブロック図である。

【図3】本発明の第1の実施形態に係るデータ改竄防止方法における処理の流れを示すフローチャートである。

【図4】本発明の第1の実施形態に係るデータ改竄防止方法の説明図である。

【図5】本発明の第2の実施形態に係るデータ改竄防止装置の構成を示すブロック図である。

【図6】本発明の第2の実施形態に係るデータ改竄防止方法における処理の流れを示すフローチャートである。

【図7】本発明の第3の実施形態に係るデータ改竄防止装置の構成を示すブロック図である。 20

【図8】本発明の第3の実施形態に係るデータ改竄防止装置における処理の説明図である。

【図9】本発明の第3の実施形態に係るデータ改竄防止方法における処理の流れを示すフローチャートである。

【図10】本発明の第4の実施形態に係るデータ改竄防止装置の構成を示すブロック図である。

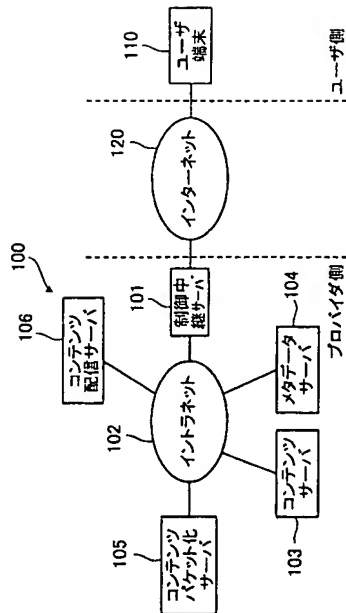
【図11】本発明の第4の実施形態に係るデータ改竄防止方法における処理の流れを示すフローチャートである。 30

【符号の説明】

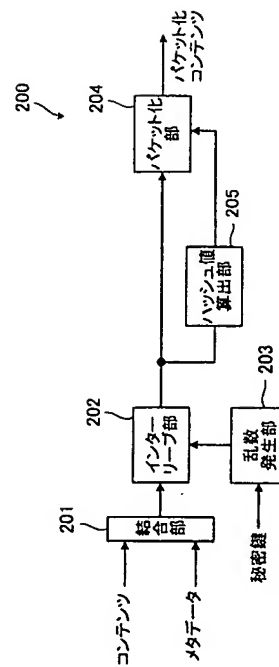
100	データ改竄防止システム	
101	制御中継装置	
102	イントラネット	
103	コンテンツサーバ	
104	メタデータサーバ	
105	コンテンツパケット化サーバ	
106	コンテンツ配信サーバ	
110	ユーザ端末	
120	インターネット	
200、700	データ改竄防止装置（コンテンツパケット化サーバ）	40
201	結合部	
202、503、703、1001	インターリーブ部	
203、504、704、1002	乱数発生部	
204、702	パケット化部	
205、501、701、1004	ハッシュ値算出部	
410	入力データ（配列入替データ）	
411	ハッシュ値の算出に用いるデータ部分	
412、811	演算対象のデータ列の一例	
420、820	ハッシュ値	
430、830	出力データ	50

4 3 1、8 3 1 変換後のデータ列
 5 0 0、1 0 0 0 データ改竄防止装置
 5 0 2、1 0 0 5 逆パケット化部
 5 0 5、1 0 0 3 メタデータ分離部
 8 1 0 入力コンテンツ

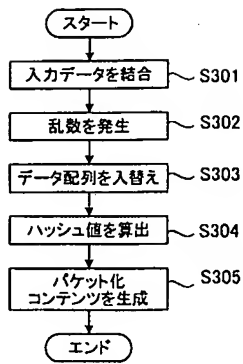
【図 1】



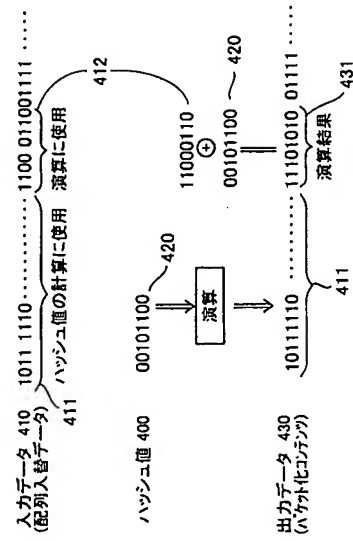
【図 2】



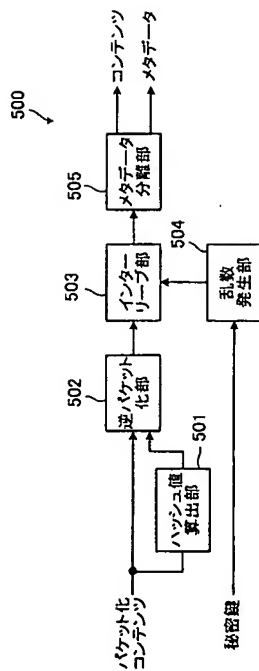
【図 3】



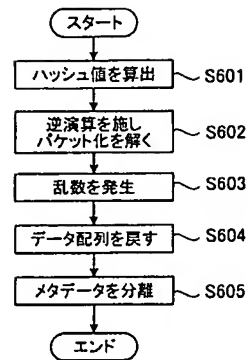
【図 4】



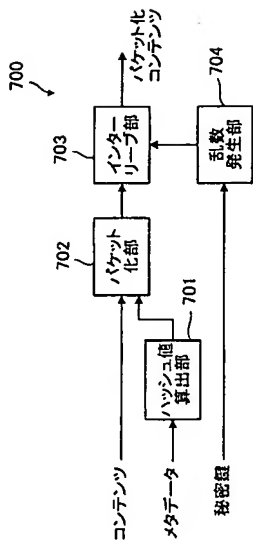
【図 5】



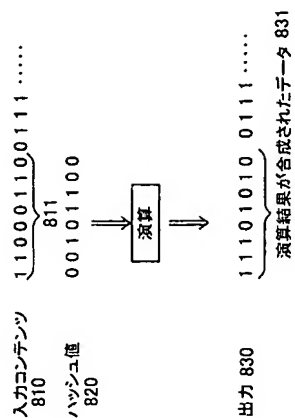
【図 6】



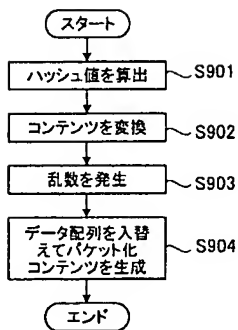
【図 7】



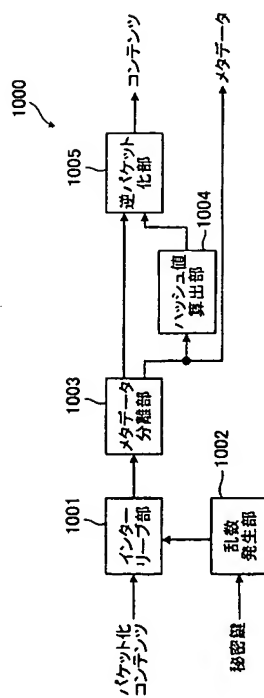
【図 8】



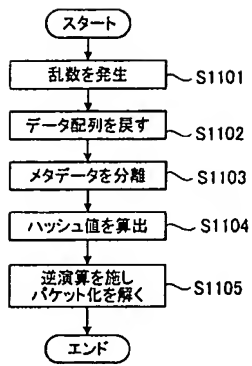
【図 9】



【図 10】



【図 11】



フロントページの続き

(72)発明者 大竹 剛

東京都世田谷区砧一丁目10番11号 日本放送協会 放送技術研究所内

Fターム(参考) 5C063 AB03 AB05 AC01 AC10 CA23 DA07 DA13

5J104 AA08 AA13 JA01 JA03 LA01 LA02 LA05 NA09 NA10 NA12

PA14